UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Susan M. Pearson, Plaintiff, v. MidWestOne Bank, Defendant.	Case No. 24-cv-01495-JWB-DTS **AMENDED AND SUPPLEMENTAL COMPLAINT WITH JURY TRIAL DEMAND**

PRELIMINARY STATEMENT

1. An unknown person or persons fraudulently induced Plaintiff to install applications on her cell phone and laptop that allowed the fraudsters to access Plaintiff's devices, and hence her checking account.

2. The fraudsters then made electronic fund transfers from Plaintiff's checking account that Plaintiff did not authorize and from which Plaintiff derived no benefit.

3. Federal consumer protection laws, including the Electronic Fund Transfer Act and its implementing regulation, impose duties on financial institutions to help protect consumers from unauthorized electronic charges to their checking accounts.

4. In enacting the Electronic Fund Transfer Act, Congress noted, "The primary objective of this subchapter … is the provision of individual consumer rights."

5. The Electronic Fund Transfer Act provides an error-resolution mechanism and limitations on consumer liability for unauthorized electronic transactions on checking accounts; such provisions are closely analogous to the provisions in the Truth in Lending Act (and its subpart, the Fair Credit Billing Act), for credit cards.

6. Before the enactment of such laws, consumers could be held liable for any losses incurred from unauthorized transactions before the consumer had notified the financial institution.

7. Before such statutory limitations on consumer liability, "there was 'little incentive' for [financial institutions] to 'take precautionary action' because any such liability could 'always be passed on to the [consumer].'" *Krieger v. Bank of America, N.A.*, 890 F.3d 429, 434 (3d Cir. 2018) (discussing Fair Credit Billing Act and quoting S. Rep. No. 91-739 at 2 (1970)).

8. Enforcement of such laws is necessary to provide the necessary incentives for financial institutions.

9. Even after Plaintiff promptly followed all of Defendant's instructions for reporting the unauthorized transactions, Defendant failed to conduct a reasonable investigation or to credit Plaintiff's account.

10. This action for damages is based on Defendant's failure to reasonably investigate and correct fraudulent and unauthorized electronic fund transfers out of Plaintiff's

checking account after being notified of the errors, and failure to limit Plaintiff's liability for unauthorized transactions on her checking account.

PARTIES

11. Plaintiff Susan M. Pearson is a natural person who resides in Minnesota, and is a "consumer" as that term is defined by 15 U.S.C. § 1693a(6) and 12 C.F.R. § 1005.2(e).

12. Defendant MidWestOne Bank ("MidWestOne") is a bank that does business in Minnesota and is a "financial institution" as that term is defined by 15 U.S.C. § 1693a(9) and 12 C.F.R. § 219.2.

FACTUAL ALLEGATIONS

13. In mid-December 2023, Plaintiff was preparing to close on the purchase of a modest home to realize her and her husband's dream of home ownership.

14. Plaintiff and her husband were at that time living in a rented bedroom in someone else's home.

15. Plaintiff and her husband had already signed a purchase agreement for their new home.

16. In about early December, 2023, Plaintiff was told by telephone that she would need approximately $18,000 for closing.

17. The money for closing could not be paid with a credit card.

18. Ms. Pearson had saved nearly $20,000 in her checking account at MidWestOne, most of which was committed to the upcoming December 22, 2023, closing on the home purchase.

19. On Friday, December 15, 2023, Plaintiff noticed several charges to one of her credit card accounts for Apple purchases that she did not make.

20. Plaintiff immediately took steps to address the false charges: that same day, December 15, 2023, she tried to call Apple Support, but was unable to speak with a representative, as she did not have an Apple account.

21. She then Googled "live Apple support" or a similar term, and a link to "Global Alive Teq" website was the top hit on her page.

22. She called the support number on that page, (833) 382-4040, which she believed was a telephone number for tech support for Apple, from whom the mysterious purchases allegedly were made, or for an Apple affiliate.

23. Unbeknownst to Plaintiff at the time, (833) 382-4040 was not really a telephone number for Apple or an affiliate; it was fraudulently represented as such on the fraudulent website.

24. Plaintiff's telephone call was answered by an imposter posing as a representative of tech support and identifying himself as "Steve."

25. "Steve" had Plaintiff add his number into her phone as "Steve from Apple."

26. The imposter fraudulently represented to Plaintiff that for him to help her figure out how the purchases had been made using Plaintiff's account, Plaintiff would first have to download an application called "Anydesk" to her Android phone and another application called "Ultraviewer" to her laptop.

27. Based on the imposter's fraudulent representations, Plaintiff downloaded the two applications.

28. Both of those applications allowed the imposter or his accomplices to remotely access Plaintiff's devices.

29. Imposter "Steve" represented that he could tell that Plaintiff supposedly had been scammed via unsecured Wi-Fi in Plaintiff's home, but that he could help her.

30. "Steve" represented that he could tell that Plaintiff's debit card for her checking account supposedly had been compromised since Oct. 27.

31. Plaintiff had previously been the victim of a fraudulent attempt to access her checking account.

32. Because Plaintiff knew from her prior experience that fraudsters will attempt to gain access to consumer's checking accounts, Plaintiff was particularly alarmed to hear "Steve" say that her debit card for her checking account supposedly had been compromised since Oct. 27.

33. Because Plaintiff needed the funds in her checking account for the impending closing, Plaintiff felt a sense of urgency and was particularly anxious to have her checking account secured as soon as possible.

34. Once the fraudster had gained access to Plaintiff's devices, and while still on the phone with Plaintiff, "Steve" had her log into her personal checking account at MidWestOne.

35. "Steve" stated that he needed to clone the transactions in order to help her and that he could see someone was trying to take a significant amount of money from her bank account.

36. Then, using Plaintiff's devices and Plaintiff's MidWestOne checking account, "Steve" or his accomplices made unauthorized electronic funds transfers from Plaintiff's checking account as follows:

- $2,239.92 at Original Technology Limited
- $2,463.93 at Original Technology Limited.

37. Original Technology Limited is a Chinese electronics store website.

38. The fraudsters' purchases from Original Technology Limited were made without Plaintiff's authorization.

39. Plaintiff received no benefit from the purchases from Original Technology Limited.

40. The two unauthorized transfers effectively drained Plaintiff's checking account, as she was left with insufficient funds for the closing, to which she had already committed.

41. When Plaintiff saw the unauthorized transfers to Original Technology Limited appear on her checking account online, she realized that she had been scammed.

42. The sort of imposter scam to which Plaintiff fell victim is well-known to industry, but not to vulnerable consumers such as Plaintiff.

43. MidWestOne was aware of suspicious activity on Plaintiff's account, but nevertheless allowed the Original Technology Limited fund transfers to go through.

44. Plaintiff contacted MidWestOne to report the unauthorized electronic fund transfers.

45. Plaintiff explained to MidWestOne exactly what happened, including that the fraudsters had fraudulently gained access to Plaintiff's devices to make the unauthorized transfers.

46. MidWestOne advised Plaintiff that she should file a police report.

47. MidWestOne suspended Plaintiff's access to her checking account.

48. MidWestOne told Plaintiff that since her phone and computer were compromised, MidWestOne needed to make sure the devices were safe before giving Plaintiff access to her checking account.

49. On December 18, 2023, per MidWestOne's instructions, Plaintiff paid to have her phone and computer scanned and for the removal of the applications that allowed remote access.

50. On December 19, 2023, Plaintiff filed a police report, as MidWestOne had instructed.

51. Because MidWestOne had suspended Plaintiff's access to her checking account, Plaintiff could not see, at the time she made the police report, the precise amounts of the two Original Technology Limited transfers.

52. Plaintiff recalled that each transfer was for $2,000 and change, but that neither transfer was for a round number dollar amount.

53. The police officer made Plaintiff feel that she had to say precise dollar and cent amounts for the unauthorized transfers.

54. Plaintiff gave the police officer precise dollar and cent amounts that she knew were in the ballpark and that she believed at that time could have been the actual precise amounts of the transfers.

55. The dollar and cent numbers Plaintiff gave the police officer were indeed quite close to, but not exactly, the actual precise amounts of the transfers.

56. When Plaintiff received her bank statement showing the actual precise amounts of the transfers, she promptly provided it to the police officer, who attached it to and made it part of his ultimate written report.

57. Plaintiff made her police report to the Forest Lake Police Department.

58. Under Minn. Stat. § 609.505, the filing of the police report would have subjected Plaintiff to criminal penalties relating to the filing of false information if, in fact, the information she reported had been false.

59. The Forest Lake Police Department opened an investigation and forwarded Plaintiff's report to the FBI.

60. Police determined that the Global Alive Teq website was suspicious, and noted as much in the December 19, 2023, incident report.

61. Police further determined that the Global Alive Teq IP address routed to India, and noted as much in incident report.

62. On December 19, 2023, Plaintiff provided MidWestOne with the name of the Forest Lake Police officer handling the case and the case number.

63. Plaintiff offered to provide MidWestOne with further information from the police.

64. MidWestOne did not take Plaintiff up on her offer.

65. On December 27, 2023, Plaintiff received a call from MidWestOne.

66. MidWestOne's representative stated that they had made a decision on the dispute: they would not credit any funds back to Plaintiff's account.

67. MidWestOne's representative stated that their decision was because the fund transfers supposedly had been authorized by Plaintiff, by one or more text messages supposedly from her.

68. Plaintiff reminded MidWestOne's representative that the fraudsters had access to Plaintiff's computer and cell phone at the time, and that MidWestOne had acknowledged as much when MidWestOne had insisted that her devices be scanned before MidWestOne would again grant Plaintiff access to her account.

69. MidWestOne's representative acknowledged that the bank knew that the fraudsters had access to Plaintiff's devices and that the bank had insisted that the devices be scanned.

70. Nevertheless, MidWestOne still refused to credit any funds back to Plaintiff's account.

71. Plaintiff received a letter from MidWestOne dated December 22, 2023.

72. MidWestOne's December 22 letter stated:

> "We have completed our research regarding your dispute and have determined that no error occurred. Customer Authorized Transaction. Please be aware that you have the right to request copies of the documents, if there are any available, that we relied on to make our determination."

73. MidWestOne's "research" did not include reviewing the police incident report.

74. MidWestOne's "research" did not include contacting the Forest Lake Police Department for any information it might have on the fraud scheme.

75. MidWestOne's "research" did not include contacting the FBI for any information it might have on the fraud scheme.

76. MidWestOne's "research" unreasonably relied on the fact that the electronic fund transfers supposedly had been authorized, by one or more text messages supposedly from Plaintiff.

77. MidWestOne's "research" disregarded the fact that the fraudsters had fraudulently gained access to Plaintiff's devices and thus had the ability to send text messages that were not actually from Plaintiff.

78. MidWestOne knew that the fraudsters had gained access to Plaintiff's devices: Plaintiff had explained as much when she first notified MidWestOne of the unauthorized transfers, and MidWestOne had insisted that Plaintiff have her devices scanned and the remote-access applications removed before MidWestOne would give back to Plaintiff access to her own account.

79. Per MidWestOne's letter, Plaintiff requested copies of the documents MidWestOne relied on to make its determination.

80. Before commencement of this lawsuit on March 25, 2024, MidWestOne never provided any documents to Plaintiff.

81. Plaintiff made multiple additional phone calls to MidWestOne to attempt to resolve the matter, but the bank repeatedly, persistently, and intentionally refused to credit any funds back to Plaintiff's account, despite having not reasonably concluded from the evidence available that the charges were authorized.

82. Every time Plaintiff spoke with MidWestOne, the bank gave her a different answer as to why it had made its determination.

83. In a telephone call on January 16, 2024, MidWestOne stated to Plaintiff that it did not have any documents to support its determination that Plaintiff supposedly authorized the transactions.

84. Although MidWestOne never asked Plaintiff to send the bank a copy of the police report, Plaintiff provided it to the bank anyway, on February 19, 2024.

85. Still MidWestOne did not credit the funds back to Plaintiff's account.

86. To date, MidWestOne still has not credited the funds back to Plaintiff's account.

87. Neither the alleged text messages nor any other documents supporting MidWestOne's decision have ever been provided to Plaintiff.

88. Plaintiff's emotional distress – from MidWestOne's refusal to credit the funds back to Plaintiff's account and Plaintiff's resulting financial hardship – went from bad to worse.

89. Plaintiff was barely sleeping 4 hours a night, lost her appetite, and was barely eating.

90. She was sick to her stomach daily.

91. Plaintiff could not focus on daily tasks.

92. Plaintiff and her husband began to have fights.

93. Neither of them were sleeping.

94. Plaintiff still cries at the drop of a hat.

95. As a result of Defendant's actions and omissions, Plaintiff has suffered actual damages, including without limitation loss of access to her money and emotional distress.

96. Plaintiff has suffered an injury in fact that is traceable to Defendant's conduct and that is likely to be redressed by a favorable decision in this matter.

97. At all times pertinent hereto, Defendant acted by and through its agents, servants and/or employees who were acting within the course and scope of their agency or employment, and under the direct supervision and control of the Defendant herein.

TRIAL BY JURY

98. Plaintiff is entitled to and hereby requests a trial by jury.

CAUSES OF ACTION

COUNT I
VIOLATIONS OF ELECTRONIC FUND TRANSFER ACT AND REGULATION E

99. Defendant violated the Electronic Fund Transfer Act and its implementing Regulation E in multiple ways, including without limitation by failing to reasonably investigate and correct the unauthorized electronic fund transfers, in violation of 15 U.S.C. § 1693f and 12 C.F.R. § 1005.11; failing to deliver to Plaintiff copies of any documents on which Defendant relied, in violation of 15 U.S.C. § 1693f(d) and 12

C.F.R. § 1005.11(d)(1); and failing to limit Plaintiff's liability, in violation of 15 U.S.C. § 1693g and 12 C.F.R. § 1005.6.

100. As a result of Defendant's violations of EFTA and Reg. E, Plaintiff has suffered actual damages, including without limitation loss of access to her money and emotional distress. Plaintiff is therefore entitled to recover actual damages pursuant to 15 U.S.C. § 1693m(a)(1).

101. Defendant is liable for statutory damages pursuant to 15 U.S.C. § 1693m(a)(2).

102. Defendant knowingly and willfully concluded that Plaintiff's account was not in error when such conclusion could not reasonably have been drawn from the evidence available to Defendant at the time of its investigation, and Defendant is therefore liable for treble damages under 15 U.S.C. § 1693f(e).

103. Defendant is liable for Plaintiff's costs and attorney's fees, pursuant to 15 U.S.C. § 1693m(a)(3).

WHEREFORE,

Plaintiff prays that judgment be entered against this Defendant for:

a.) Plaintiff's actual damages, including unliquidated damages in an amount greater than $50,000;

b.) Statutory damages of $1,000 pursuant to 15 U.S.C. § 1693m(a)(2);

c.) Treble damages pursuant to 15 U.S.C. § 1693f(e);

d.) Reasonable costs and attorney's fees pursuant to 15 U.S.C. § 1693m(a)(3);

e.) Such other and further relief as may be just and proper.

Dated: 11/13/24

GOOLSBY LAW OFFICE, LLC

By: s/John H. Goolsby

John H. Goolsby, #0320201
475 Cleveland Ave. N, Suite 212
Saint Paul, MN 55104
Telephone: (651) 646-0153
jgoolsby@goolsbylawoffice.com
Attorney for Plaintiff